

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA

v.

GREGORY COLBURN, et al.,

Defendants.

No. 19-CR-10080-NMG

MOTION TO SUPPRESS THIRTEEN “CONSENSUAL WIRETAP” CALLS

For the reasons set forth below, Defendants Gamal Abdelaziz and John Wilson respectfully request that the Court suppress thirteen “consensual wiretap” calls. It has come to Defendants’ attention that the government made a profound error in the manner in which the “consensual wiretap” calls in this case were recorded. In short, the government had AT&T continue to monitor Rick Singer’s phone for nearly five months *after* the valid court order authorizing the wiretap expired. The government enlisted AT&T’s assistance not with any lawful authority, as required by statute, but pursuant to a misdated letter from former AUSA Eric Rosen that attached a “consent form” providing Mr. Singer’s agreement that the government could monitor a phone *different* than the phone AUSA Rosen requested that AT&T monitor.

BACKGROUND

As set forth in the discovery provided by the government in this case, Judge Burroughs authorized four wiretaps in this matter pursuant to 18 U.S.C. § 2510 *et seq.* Wiretap applications were sworn before Judge Burroughs and orders were issued on the following dates: June 5, 2018; July 3, 2018; August 2, 2018; and August 30, 2018.

On October 2, 2018, former AUSA Eric Rosen filed an application to seal the last set of recordings and postpone the inventories.¹ That application (attached hereto as Exhibit A) stated:

The monitoring of TARGET TELEPHONE 1 began on August 30, 2018 and ceased at midnight of September 27, 2018. The government's investigation of this matter continues in that SINGER is now cooperating with investigators and he is placing consensual calls to various target subjects.

What AUSA Rosen concealed from the Court was that Singer was not “placing consensual calls” in the traditional manner (i.e., on a government phone, through use of a government-issued recording device, in government offices, or through the use of government-issued recording software). Indeed, the “monitoring of TARGET TELEPHONE 1” **did not cease** at midnight of September 27, 2018 as represented to the Court. Instead, by letter dated September 20, 2018 (attached as Exhibit B), AUSA Rosen had separately contacted and requested that AT&T **continue** the wiretap of Singer's phone past the expiration date of the Court's Order on the representation that Singer had consented to such monitoring. AT&T obliged and continued to conduct electronic surveillance on Mr. Singer's phone for almost **five additional months** without a valid court order authorizing such monitoring. All of the so-called “consensual calls” that are at issue in this case were intercepted in this manner.

Attached to the government's recent Motion for Authentication of Records (Dkt. 2099) is the Declaration of FBI Supervisory Special Agent Jaamal C. King, who is a member of the Telecommunications Intercept & Collection Technology Unit in Quantico, VA (Dkt. 2099-1). Agent King's affidavit confirms that the “wire” was up on Mr. Singer's phone from June 5, 2018 to March 14, 2019 **despite AUSA Rosen's representation that “monitoring ceased at midnight of September 27, 2018.”** In other words, there was no “break” between Judge

¹ All documents appear to have been filed in No. 18-MC-91232-ABD. The undersigned do not have access to the full docket but have been provided selected documents by the government.

Burroughs's authorization of the electronic surveillance pursuant to Court order and AUSA

Rosen's self-authorization of the continued electronic surveillance through his letter to AT&T.

Agent King further explained how the wiretap in this case worked:

The authorized surveillance in this case includes those collections performed through the assistance of a wireless telecommunications service provider (Provider) pursuant to the Communications Assistance for Law Enforcement Act (CALEA). CALEA requires providers to have the ability to perform electronic surveillance **pursuant to a court order or other lawful authorization.** Under the CALEA model, the provider performs the authorized intercept while providing the communication to law enforcement for collection.

(emphasis added). In layman's terms, AT&T did all of the work and handed off to the government the content of all of the telephone calls. It is telling that Agent King's declaration states that interceptions can only be made pursuant to a "court order" or "lawful authorization," because AUSA Rosen's letter to AT&T was neither.

AUSA Rosen's letter to AT&T was dated September 20, 2018, although it is unclear when it was actually sent. The letter is titled "Consensual Monitoring of Wireless Phone by Law Enforcement" and states, in part:

Kindly accept this correspondence as confirmation of representations made by the Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI) regarding the consensual monitoring of mobile phones for law enforcement purposes pursuant to 18 U.S.C. § 2511(2)(c). The specific phone referenced in this letter for AT&T's assistance in conducting consensual monitoring is an AT&T cellular telephone assigned telephone number [] 8802.

...

After a thorough review of current applicable law, it is the position of the DOJ/FBI that an order is not required when a party to a communication consents to the monitoring, even when that phone used is inherently mobile; however, since DOJ/FBI also recognizes the rights of third parties should be protected, the consenting party will be required to read and sign a statement pledging that the phone shall not be used by any other party. . . . Thank you for your anticipated cooperation in this matter.

Despite the reference to “a thorough review of current applicable law,” no authority is cited. AUSA Rosen’s letter to AT&T attached a “Consent and Acknowledgment” executed by Rick Singer on September 27, 2018 (in other words, seven days **after** the date of AUSA Rosen’s letter).² That form (attached as Exhibit C) stated, in part:

I consent to the interception and recording of any and all communications made by me over all telephones, cellular or otherwise, **provided to or made available to me by law enforcement agents in connection with actions taken by me in connection with law enforcement agents.**

(emphasis added). The problem with Mr. Singer’s purported consent, however, is that the telephone that AUSA Rosen asked AT&T to monitor (ending 8802) was **Mr. Singer’s personal phone**. Mr. Singer’s consent only applied to phones “provided to or made available to” him by law enforcement in connection with law enforcement investigations and did not extend to his personal phone. AUSA Rosen apparently misled AT&T into believing that there was written consent to monitor the phone number ending in 8802 when in fact there was no such consent.³ AT&T’s agreement to continue the electronic surveillance for five months past the expiration of the Court order was therefore predicated on a faulty representation made to the Company by the Department of Justice.

ARGUMENT

I. Regardless of Consent, A “Wire” Provider Cannot Assist in Interception And Monitoring Absent Court Order Or Other Lawful Authority

As Agent King stated, wire providers can assist in intercepting and monitoring telephone calls “pursuant to a court order or other lawful authorization.” AUSA Rosen’s letter was neither.

² The undersigned do not know why the letter was backdated or when the letter was actually sent.

³ As further set forth in the March 2020 prosecutorial misconduct briefing in this case, the FBI did provide Mr. Singer with a phone, but the FBI-provided phone was unmonitored. Mr. Singer was instructed to use the FBI-provided phone (which former AUSA Rosen appeared to refer to as a “burner,”) when speaking with the AUSAs and the FBI precisely because those phone calls would **not** be recorded

The consensual monitoring provision upon which the AUSA Rosen purported to base his letter request to AT&T is 18 U.S.C. § 2511(2)(C). That provision states:

It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

This section allows law enforcement officers and confidential informants to use traditional methods of interception, such as government phones, tape recording devices, and tape recording software, to monitor and intercept telephone calls where only one party to the phone call consents to such monitoring and interception. It would have been entirely appropriate for the government to rely on this provision if they had provided Mr. Singer with a government phone and equipped it with a recording device, or even if they permitted Mr. Singer to keep his own phone and gave him a recording device to use. But that is not what happened. As noted above, the electronic surveillance was done by AT&T at AUSA Rosen's request.

What the government ignored is that § 2511(2)(C) does not apply to a wire "provider" such as AT&T. A different section, 18 U.S.C. § 2511(2)(a)(ii), specifically refers to "providers of wire or electronic communication service" and states:

Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents . . . are authorized to provide information, facilities or technical assistance to persons authorized by law enforcement to intercept wire, oral, or telephonic communications If such provider, its officers, employees, or agents . . . has been provided with – (A) a court order directing such assistance . . . or (B) a certification [of an "emergency situation"], setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required.

The above provision is the only provision in the United States Code that authorizes telephone providers such as AT&T to assist law enforcement in intercepting telephonic

communications under Title III.⁴ According to the plain language of the statute, AT&T cannot assist law enforcement in intercepting telephonic communications without either (1) a court order; or (2) a certification of an “emergency situation.” There is no exception for a law enforcement request where consent is provided pursuant to 18 U.S.C. § 2511(2)(C). In this case, no court order was obtained. Nor was there any certification of an “emergency situation.” Therefore, AT&T was not authorized to maintain the “wire” on Singer’s personal phone, whether or not Singer provided adequate consent (and he did not). AUSA Rosen’s pronouncement that “after a thorough review of current applicable law, it is the position of the DOJ/FBI that an order is not required when a party to a communication consents to the monitoring,” cannot change the plain language of the statute. *See In re Application of United States.*, 128 F. Supp. 3d 478, 482 (D.P.R. 2015) (“Of the two Title III provisions cited by the government, § 2511(2)(a)(ii) authorizes **providers** to furnish assistance in accordance with a court order or a certification § 2511(2)(c) simply authorizes **law enforcement** to conduct wiretaps without court approval where permission is given by one party to the communication.”) (emphasis added). *Cf. United States v. Rodriguez*, No. 17-CR-10066-IT, 2018 WL 988054, at *4 (D. Mass. Feb. 20, 2018) (“It is for the court, and not the service provider, to decide whether interception is warranted.”).

⁴ A general prohibition is also found in 47 U.S.C. § 605(a): “Except as authorized by chapter 119, title 18, no person receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate . . . communication by wire . . . shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception, (1) to any person other than the addressee, his agent, or attorney, (2) to a person employed or authorized to forward such communication to its destination, (3) to proper accounting or distributing officers of the various communicating centers over which the communication may be passed, (4) to the master of a ship under whom he is serving, (5) in response to a subpoena issued by a court of competent jurisdiction, or (6) on demand of other lawful authority.”

This requirement that a “wire” provider receive a court order is set forth in the original legislative history that added what is now 18 U.S.C. § 2511(2)(a)(ii). According to the House Report:

This provision would ... require the Government to provide a copy of the Attorney General certification [of emergency need] or portions of the court order and other information to the person rendering assistance. . . . **Requiring the court order or certification to be presented before the assistance is rendered places an additional obstacle in the path of unauthorized surveillance activity** The Court order or certification must indicate the period of time during which the provision of information, facilities or technical assistance is authorized and must specify the information, facilities or technical assistance required. [These requirements] will eliminate any doubts the party providing assistance might harbor concerning what is required of him and what are the limits of his authority.

H.R. Rep. No. 95-1283, pt. 1, at 98-99 (1978) (emphasis added). Although at first glance it may seem odd to require a telephone company to receive a court order prior to intercepting a telephone where the owner of the device has already consented to such interception, there is very good reason for this rule. That is: **there is an enormous difference between traditional methods of consensual recording and a so-called “consensual wiretap.”** With traditional methods, the recording is limited by the fact that either the government or the informant must physically record each call. Usually this is either done at the government’s offices, or the informant is given a recording device to use when he speaks with persons of interest. The informant can—in effect—revoke consent whenever he would like because he can simply stop recording or stop cooperating with law enforcement. And there is hardly any risk that the recordings will capture a phone call in which neither party has consented to recording—which would be illegal—if the informant let someone else use his phone, because either the informant or the government control each recording.

When law enforcement has the phone company’s technical assistance, however, they are granted the “keys to the castle” because the phone company can set up an actual,

traditional wiretap, intercept all calls, and provide the recordings directly to law enforcement with little or no informant interaction and no court authorization. *See* Agent King’s Declaration. In Mr. Singer’s case, this meant that electronic surveillance was ongoing for nearly five months after the last court order expired, capturing **every single call** going in and out of Mr. Singer’s cell phone. Unlike a traditional wiretap, there were no “minimization” procedures and no agent to constantly monitor the line and ensure that non-targets were not being recorded. *See United States v. Lopez*, 300 F.3d 46, 57 (1st Cir. 2002) (“The minimization requirement ‘spotlights the interest in confining intrusions as narrowly as possible so as not to trench impermissibly upon the personal lives and privacy of wiretap targets and those who, often innocently, come into contact with such suspects.’”). And the wiretap was apparently never-ending, because AT&T was not provided with an order setting forth “the period of time during which the provision of the information, facilities, or technical assistance is authorized” as is required by 18 U.S.C. § 2511(2)(a)(ii).

It is easy to see why Congress would demand that, in these circumstances, telephone companies can only provide assistance to law enforcement if they are ordered to do so by the court. The requirement of a court order ensures that law enforcement cannot enlist the assistance of telephone companies to set up intrusive wiretaps simply on a particular AUSA’s “say so.” Congress could have easily imagined a situation in which a rogue agent enlisted the assistance of the telephone company to set up a wire, stating that he or she has legal authority (such as consent) when in fact he or she has no such authority. Without the requirement of a court order, the possibilities for abuse are endless. *See Lopez*, 300 F.3d at 57 (to determine whether government has fulfilled its obligation to minimize unauthorized communications under a “standard of honest effort,” courts consider “the nature and complexity of the suspected crimes,”

“the thoroughness of the government’s precautions to bring about minimization;” and “the **degree of judicial supervision** over the surveillance process”) (emphasis added). *Cf. United States v. Hoffman*, 832 F.2d 1299, 1306-07 (1st Cir. 1987) (“[I]n a society which values privacy and the rights of the individual, wiretapping is to be distinctly the exception—not the rule.”).

The necessity of having a judicial officer mediate between law enforcement and the phone company—even where there is consent under 18 U.S.C. § 2551(2)(C)—is present in this very case. As noted above, AUSA Rosen told AT&T that Singer provided consent to monitor his personal phone number, but in fact the consent AUSA Rosen procured (and provided to AT&T) was for something different—the recording of a phone *provided by law enforcement*. If AUSA Rosen had followed proper procedures and brought the matter to the Court before enlisting AT&T’s assistance, surely Judge Burroughs would have recognized the error and ordered it to be corrected before AUSA Rosen made a false representation about Singer’s consent to AT&T. The system set up by Congress—with a judicial “check” on the government’s ability to compel telephone companies to provide assistance—would have worked as intended.

It is not clear why AUSA Rosen did not follow the procedure established under law. To be sure, it would not have been very difficult for AUSA Rosen to obtain a court order compelling AT&T to continue to provide assistance in intercepting Singer’s calls. Indeed, when AUSA Rosen went back to Judge Burroughs to seal the lawfully-acquired wiretap tapes, there is no reason that he could not have filed a simple application for a court order explaining that Singer had consented, attaching the consent form, and providing a short background statement on what he wished to gain from the interceptions. If Singer had provided valid consent, AUSA Rosen need not have followed the entire 18 U.S.C. § 2518 process. *See In re Application of United States*, 128 F. Supp. 3d at 482 (“Notably, while § 2511(2)(a)(ii) authorizes providers to furnish

assistance upon a court order, it does not explicitly state that the order be one pursuant to § 2518.”). Indeed, “court orders under § 2511(2)(a)(ii) are distinct from interception orders pursuant to § 2518, which must include additional information.” *Id.*

II. Singer Did Not Grant Consent

The government committed not one but two critical errors in the way it handled the so-called “consensual” wiretap. As noted above, the “consent form” that Rick Singer signed permitted law enforcement to monitor any phone “provided to or made available to me by law enforcement agents in connection with actions taken by me in connection with law enforcement agents [sic].” *See* Ex. C. But AUSA Rosen had AT&T monitor Singer’s personal iPhone, which was **not** the phone that was provided to him by law enforcement. In fact, AUSA Rosen had it backwards. He provided Singer with a mobile phone but did **not** monitor the law enforcement phone, and specifically told Singer to use the unmonitored phone to call law enforcement precisely because there would be no record of those calls. **In other words, the phone for which there was not consent was monitored, and the phone for which there was consent was not monitored.**

Regardless of whether AUSA Rosen obtained the required court order, therefore, the “consensual wiretap” independently violated Title III because there was no valid consent. The fact that Singer did not consent to the monitoring of his personal phone is confirmed by a letter AUSA Rosen wrote to counsel (and to Magistrate Judge Kelley) on February 26, 2020. In that letter, AUSA Rosen asserted that the infamous iPhone “notes” in which Singer recounted that the agents encouraged him to lie were not provided to defense counsel as *Brady* (a decision this Court later found was “irresponsible and misguided”)⁵ because “the government believed the

⁵ Dkt. 1169 at 8.

notes were privileged.” Clearly, even the government had mistaken which telephone Singer had given consent to monitor. After all, if Singer had actually consented to the government monitoring his personal iPhone, AUSA Rosen’s assertion that anything on that phone could be privileged would be patently absurd.

In short, Singer did not consent to the monitoring of his personal iPhone. And to the extent the government might argue that he provided implied consent, the Court should hold an evidentiary hearing to make a determination on that issue.

III. The Remedy is Suppression

In light of the foregoing, Singer’s so-called “consensual wiretaps” from September 28, 2018 to March 14, 2019 were tainted by violations of 18 U.S.C. § 2510 *et seq.* Defendants Abdelaziz and Wilson are “aggrieved persons” because they were parties to thirteen such wires which were both “unlawfully intercepted,” 18 U.S.C. § 2518(10)(a)(i), and for which “the order of authorization or approval under which it was intercepted is insufficient on its face.” 18 U.S.C. § 2518(10)(a)(ii). The government’s failure to obtain a court order authorizing the wiretap as required by 2511(a)(ii) is a failure to satisfy a statutory requirement that “directly and substantially implement[s] the Congressional intention to limit the use of intercept procedures to those situations clearly calling for the employment of this extraordinary investigative device.” *United States v. Giordano*, 416 U.S. 505, 527 (1974). Thus, the thirteen recordings with Abdelaziz and Wilson therefore must be suppressed under 18 U.S.C. § 2515. *See Giordano*, 416 U.S. at 524-29. To the extent Singer did not consent to the wiretaps, they also must be suppressed under the Fourth Amendment.

IV. The Court Should Consider This Motion

Although the undersigned understand that the Court had previously set the deadline for pre-trial motions, they respectfully request that the Court exercise its discretion to consider this motion because there is good cause for the delay. See Fed. R. Crim. P. 12(c)(3). In particular, the nature of the government's violations of the wiretap statute were only recently fully exposed by the government's Notice and Motion Regarding Authentication (and its associated documents, including the affidavit of Special Agent King), which demonstrate that the government did not distinguish between the court-authorized electronic surveillance and the "consensual" recordings during this case. Defendants would face severe prejudice if the Court did not consider this motion because the so-called "consensual wiretaps" are critical evidence in this case and improperly obtained electronic surveillance materials should not be used at trial. Defendants further note that the government never disclosed this statutory violation and that Defendants uncovered the issue only four days ago and filed the instant Motion forthwith.

CONCLUSION

For the reasons set forth above, Defendants Gamal Abdelaziz and John Wilson respectfully request that the Court suppress the thirteen so-called "consensual wiretap" calls on which they were intercepted. To the extent the Court denies that relief, Defendants respectfully request that the Court hold an evidentiary hearing on the issue of consent.

Dated: August 31, 2021

Respectfully submitted,

GAMAL ABDELAZIZ

By his attorneys,

/s/ Brian T. Kelly

Brian T. Kelly (BBO # 549566)

Joshua C. Sharp (BBO # 681439)

Lauren M. Maynard (BBO # 698742)

NIXON PEABODY LLP

53 State Street
Boston, MA 02109
(617) 345-1000
bkelly@nixonpeabody.com
jsharp@nixonpeabody.com
lmaynard@nixonpeabody.com

Robert Sheketoff (BBO # 457340)
One McKinley Square
Boston, MA 02109
617-367-3449

JOHN WILSON

By his attorneys:

/s/ Michael Kendall
Michael Kendall (BBO # 544866)
Lauren M. Papenhausen (BBO # 655527)
WHITE & CASE LLP
75 State Street
Boston, MA 02109-1814
(617) 979-9300
michael.kendall@whitecase.com
lauren.papenhausen@whitecase.com

Andrew E. Tomback (pro hac vice)
MCLAUGHLIN & STERN, LLP
260 Madison Avenue
New York, NY 10016
(212) 448-1100
atomback@mclaughlinstern.com

LOCAL RULE 7.1(A)(2) CERTIFICATION

I hereby certify that counsel for the defendants conferred with counsel for the government in an attempt to resolve or narrow the issues raised by this motion. The government opposes this motion.

/s/ Brian T. Kelly
Brian T. Kelly

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing was filed electronically on August 31, 2021, and thereby delivered by electronic means to all registered participants as identified on the Notice of Electronic Filing.

/s/ Joshua C. Sharp
Joshua C. Sharp